ABSTRACT

A security protocol for combining user and platform authentication. The security protocol includes a first handshake phase to issue attestation identity credentials, and a second handshake phase to authenticate based on the attestation identity credentials issued in the first handshake phase. The security protocol also includes a session resumption phase to resume a previous session.